## Квадратичные вычеты

**Определение:** Зафиксируем простое число p. Для числа a, не делящегося на p, рассмотрим сравнение  $x^2 \equiv a \pmod{p}$ . Если это сравнение имеет решение, то число a называется квадратичным вычетом по модулю p, в противном случае — квадратичным невычетом по модулю p. Достаточно часто слово «квадратичный» мы будем опускать.

## Свойства:

- П Пусть p > 2. Докажите, что
  - (a) по модулю p существует ровно  $\frac{p-1}{2}$  квадратичных вычетов и столько же невычетов;
  - (b) произведение двух квадратичных вычетов вычет;
  - (с) произведение вычета на невычет невычет;
  - (d) произведение двух невычетов вычет.
- $\boxed{2}$  Докажите, что все квадратичные вычеты являются корнями многочлена  $x^{\frac{p-1}{2}}-1\in \mathbb{F}_p[x]$ , а все невычеты корнями многочлена  $x^{\frac{p-1}{2}}+1\in \mathbb{F}_p[x]$ .

**Определение:** Символом Лежандра называется выражение, обозначаемое  $\left(\frac{a}{p}\right)$ , равное 1, если a — квадратичный вычет по модулю p; равное -1, если a — невычет по модулю p и 0, если a кратно p.

Из свойств 1 и 2 следует, что  $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$ , а также  $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}\pmod{p}$ .

## Задачи:

- Пусть p=163,  $\left(\frac{a}{p}\right)$  символ Лежандра. Чему равно  $\sum_{a=1}^{p}\left(\frac{a}{p}\right)$ ?
- [2] Докажите, что если  $x^2 + 1$  делится на p, то p имеет вид 4k + 1.
- Покажите, что для каждого простого числа p существуют целые числа a и b, такие что  $a^2+b^2+1$  кратно p.
- $\boxed{4}$  Докажите, что  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ .
- [5] Решите в целых числах уравнение  $z(y^2 5) = x^2 + 1$ .
- [6] Докажите, что уравнение  $4xy x y = z^2$  (a) не имеет решений в натуральных числах; (b) имеет бесконечно много решений в целых числах.
- [7] Решите в целых числах уравнение  $x^3 + 7 = y^2$ .
- [8] Докажите, что  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ .

9 Лемма Эйзенштейна Докажите, что

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{(p-1)/2} \left\lfloor \frac{2an}{p} \right\rfloor}.$$

- 10 Четность числа  $\varepsilon(q)$  совпадает с четностью числа целых точек в треугольнике, заданном неравенствами  $0 < x < \frac{p}{2}, 0 < y < \frac{q}{2}, y < \frac{qx}{p}$
- 11 **Квадратичный закон взаимности** Для различных нечетных простых чисел имеет место равенство

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

- 12 Является ли число 74 квадратичным вычетом по модулю 131?
- 13 Целое число a таково, что  $a^2-6a+3$  делится на некоторое простое p. Докажите, что существует целое число b такое, что  $b^2-2b-53$  делится на p.
- Дано натуральное a, не делящееся на простое p. Рассмотрим перестановку чисел  $0,1,\ldots,p-1$ , на i-м месте которой стоит остаток ai от деления на p. Докажите, что эта перестановка четна при  $\left(\frac{a}{p}\right)=1$  и нечетна при  $\left(\frac{a}{p}\right)=-1$
- 15 Для простого p найдите значение выражения

$$\sum_{a=1}^{p-1} \left( \frac{a^2 + a}{p} \right)$$

16 Докажите, что для простого числа p>2 наименьший квадратичный невычет по модулю p меньше  $1+\sqrt{p}$ .